Achieve DPDP Act 2023 Compliance!

A step-by-step guide for CPG brands to India's new Digital Privacy Law.

FieldAssist

Contributors

Amit Kumar

Group Counsel, DPO (FIP, CIPPE, and CIPM)

Sowmya Vedarth

Partner, Risk Advisory at Delloite India

Varun Pandey

CTO & Chief Security Officer at FieldAssist

Shashwat Gosh

CMO at FieldAssist

You think last year was big for digital privacy?

Brace yourself for 2024, as it is all set to change the cookie-cutter approach to individual, consumer, and employee data protection!

Today, it has become imperative for FMCGs to ensure transparency and be more mindful of data collection. YOU and I, as individuals, have fundamental rights to know what information is being collected and what is happening with our information. And organizations need to safeguard consumer privacy.

India's NEW 'Digital Personal Data Protection (DPDP) Act is a momentous stride in safeguarding individual privacy rights and promoting responsible data management practices.

This groundbreaking legislation aims to balance individual rights and an organization's legitimate data-processing needs.

What will be the baseline to steer towards regulatory compliance? What swift measures need to be taken to address DPDP's potential impact? How do we balance the need for direct selling while avoiding hefty penalties?

Our Data Privacy Handbook prepares FMCGs/FMCDs for the upcoming risks, rewards, responsibilities, and what's in store to kick-start their data privacy compliance journey effortlessly.

“Decoding DPDP ACT 2023 for CPG - Webinar by FieldAssist” covers the topic in-depth, where expert panelists empower CXOs with a checklist to propel forward in 2024 while avoiding non-compliance issues and hefty legal penalties.

While awaiting final government rules, companies should anticipate a 12-month transition for DPDP compliance, barring age-gating provisions.

So, are you ready to embark on this journey? Let's delve into the framework and support India's privacy initiatives together!

What is the Digital Personal Data Protection Act 2023?

Digital Personal Data Protection (DPDP) Act 2023 is India's first-ever dedicated attempt to bring a harmonized data privacy regime.

The Act is a comprehensive framework aimed at safeguarding the privacy and security of Indian citizens' personal information by establishing strict regulations for data protection. The new law will give individuals greater control over their data and govern how businesses collect, process, store, and share their customers' personal information.

Territorial Scope

- Processing of digital personal data within the territory of India.
- Processing digital personal data outside India targeting Indian citizens concerning any activity related to offering goods and services within India.

Material Scope

- Personal data that is collected in digitized form
- Personal data collected in non-digital form and digitized subsequently

Key Stakeholders Defined in the DPDP Act

Data Processor

Person/company appointed by a Data Fiduciary to process data.

Data Fiduciary

Individual/Business/Govt. body, based in India or operating from a foreign location, who process personal data of Indian citizens to offer them goods or services.

Data Protection Board of India

Apex body in charge of the enforcement of the DPDP Act.

Data Principal

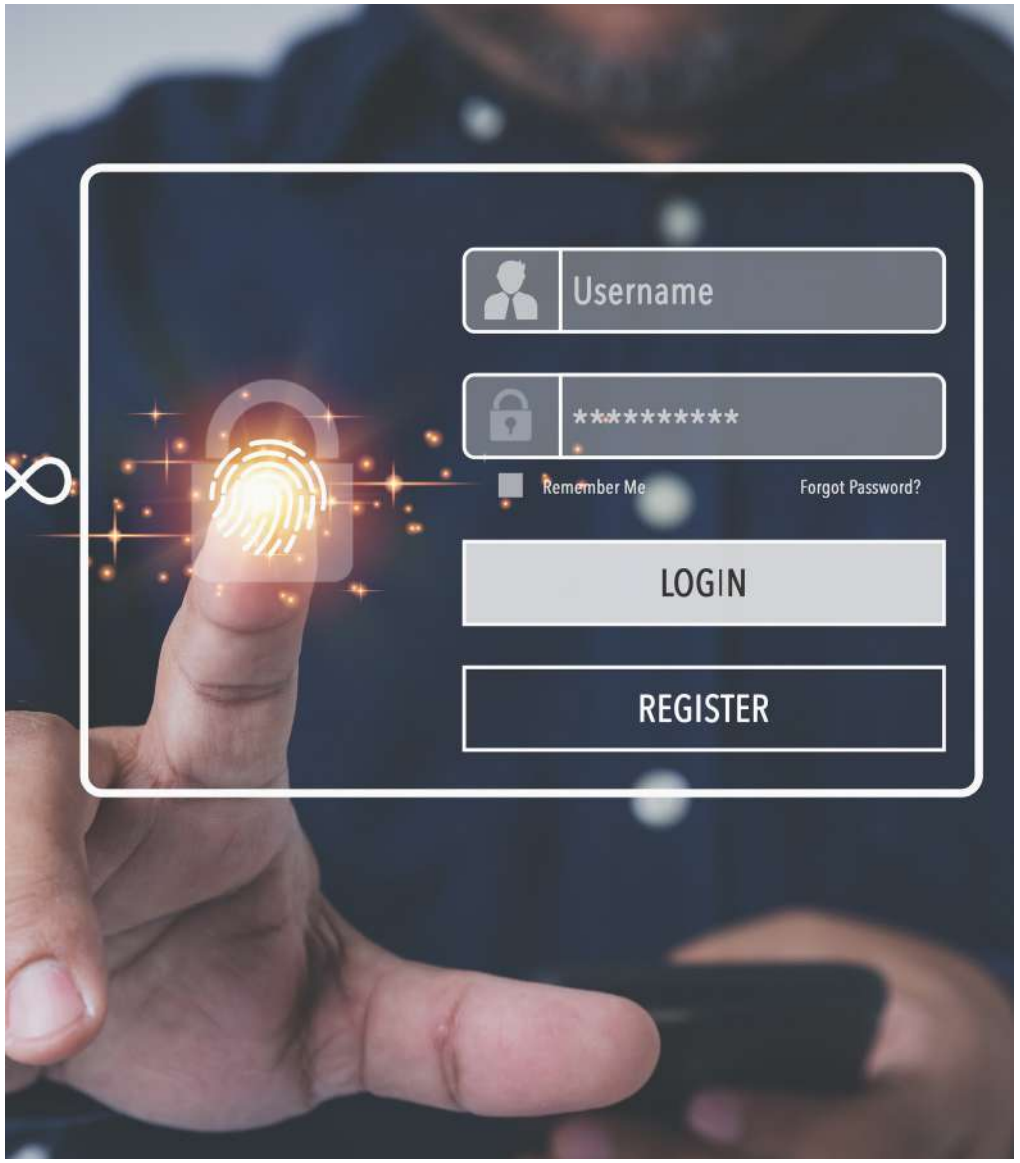
Indian citizens whose personal data is being processed

Data Protection Officer

Individual appointed by a Data Fiduciary to monitor DPDP Act compliance.

Key Highlights of the Act

- **Personal Data -** Any individual data, including name, address, contact info, medical records, bank details, or data sourced through online trackers and smart devices, directly or indirectly identifies them.
- **Child Gating Till 18 Years of Age -** Children's personal data should not be used for tracking, behavioral monitoring, or targeted advertisement.
- Extended enterprises, including third parties processing data, must comply with international standards like ISO.
- The Act also emphasizes the requirement to follow data localization and minimization and store sensitive personal data within India.
- There are financial penalties of up to **INR 250 crore** for data fiduciaries, and the Act does not impose criminal penalties for non-compliance.
- **Cross-border data transfers -** The act has eased the cross-border data transfer requirement where Data Fiduciaries can share/transfer data outside India. However, certain transfers can be restricted by the Government.



Rights of Data Principals

- Right to access personal information
- Right to consent and withdrawl of consent
- Right to correction of erasure
- Right to nominate
- Right to grievance redressal

Comparative Analysis: The India DPDP v EU GDPR

The DPDP Act draws parallels with the European Union's General Data Protection Regulation (GDPR) and incorporates several GDPR-like features, including individual consent, data subject rights, and the responsibilities of data processors and fiduciaries.

However, the DPDP Act introduces concepts like “data fiduciary” and “data principal,” bringing nuances tailored to the country’s sociocultural and economic contexts.

DPDP Act is also one of the most comprehensive laws offering a Grievance Redressal mechanism, enabling data fiduciaries to have systems in place for the timely resolution of complaints related to data processing.

India’s DPDP Act also includes child gating, allowing the brands to adopt strategies to ensure compliance with specific obligations for processing data related to children below the age of 18 years.

DPDP Act Through The Lens of Consumer Businesses

Have you ever visited a Nike website, then opened an article on another business website, and saw that the shoes you just looked at follow you everywhere?

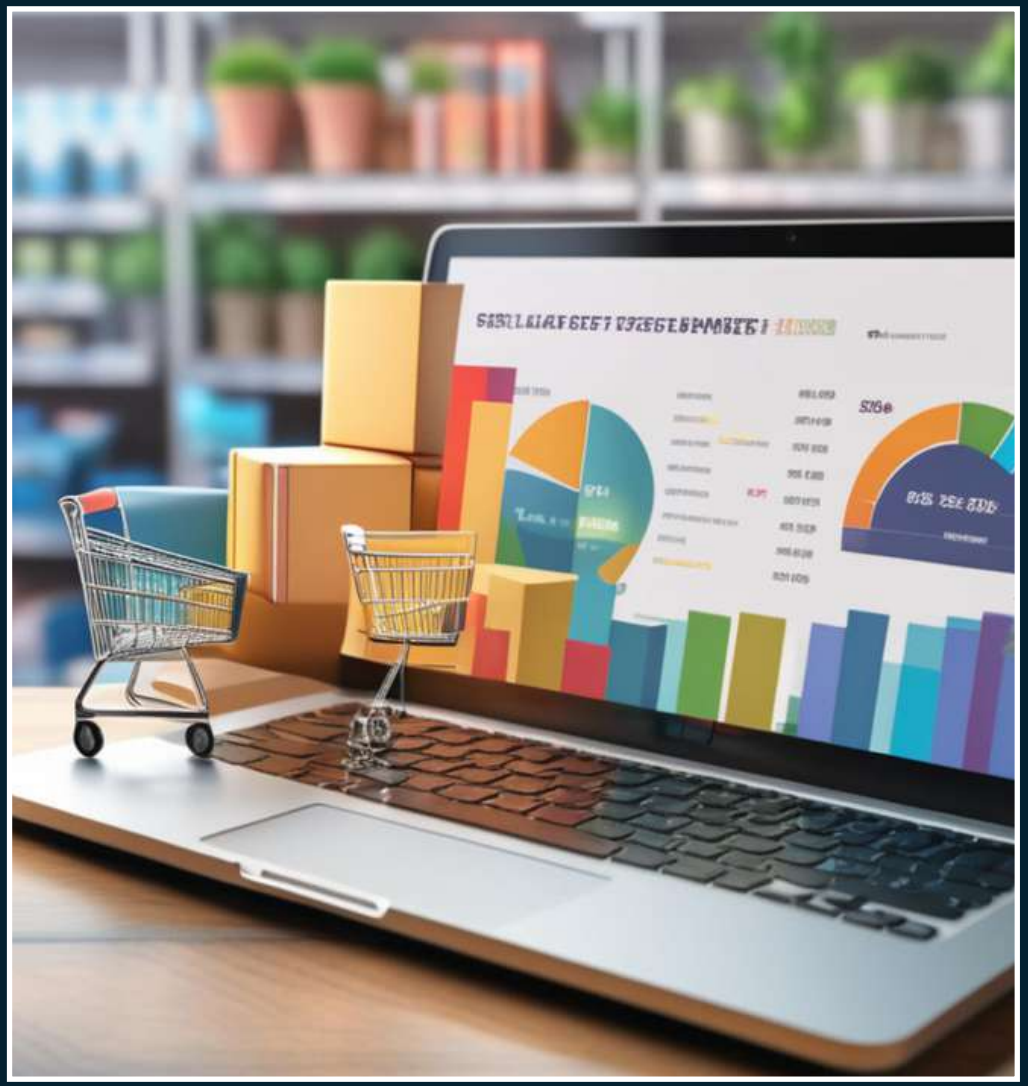
Even your fitness band knows more about you than your loved ones, irony, right?

Did you know your employer can likely track your emails, phone activity, location, productivity, and even the words you type on work devices?

What drives every retail and consumer-oriented business model these days? Personal data!

We live in a time of no shortage of data. It flows from in-store and online transactions, store technology, loyalty programs, social media, mobile operators, and other providers. As consumer data and its monetization potential grow significantly, so do the privacy challenges.

The Digital Personal Data Protection (DPDP) Act 2023 is an essential piece of legislation set to touch the lives of consumers, employees, and business owners alike.



It is expected to have a far-reaching impact on individuals, businesses, and the economy.

As a CXO, you might think we already have ISO 27,001 and a security framework. Do we still require a privacy framework? How does it change, or what does it change? YES!

Data privacy concerns are driving consumer behavior. As consumers become more careful about sharing data and regulators step up privacy requirements, FMCGs need a data protection and privacy framework to create business advantage, improve consumer engagement, and be responsible for keeping consumer data safe.

FMCG companies should not view the DPDP Act as a compliance mandate but consider this as an opportunity to enable business innovations. Adapting the consent architecture and data trust framework helps CPGs better control their data, thereby maintaining the balance between value protection and value creation while staying compliant and gaining a competitive advantage.

To do all that, enterprises need to move quickly, and they need a plan.

"Compared to 43A or SDI Rules, The DPDP Act is India's first and the most comprehensive legislation - giving You and I as individuals the power to control our data and at the same time allowing businesses to collect data for enhanced experiences."

Amit Kumar
Group Counsel, DPO
(FIP, CIPPE, and CIPM)

How can FMCGs/ FMCDs prepare for compliance?

In 2024, FMCG and FMCD companies face a crucial challenge: balancing privacy and insights. It's clear that the trend toward privacy-focused regulations and technologies is irreversible. They must adapt to thrive in this new environment.

Some of the obligations CPGs (Data Fiduciaries) have under the act:

Obligations of Data Fiduciaries:

- Implement technical and organizational measures to safeguard personal data
- Ensure lawful, fair, and transparent usage of data
- Notify purpose and seek consent from Data Principals where required
- Keep storage limited only to a fixed duration
- Protect personal data when transfering overseas
- Implement a mechanism for Data Principals to exercise their rights
- Keep usage limited to the purpose of collection
- Implement a grievence redressal mechanism for handling queries from Data Principals
- Have a breach management policy in case of confidentiality breach
- Hire right data processors to ensure key obligations are abided by, including timely deletion of data

The DPDP Act defines a new term - **'Significant Data Fiduciary'**

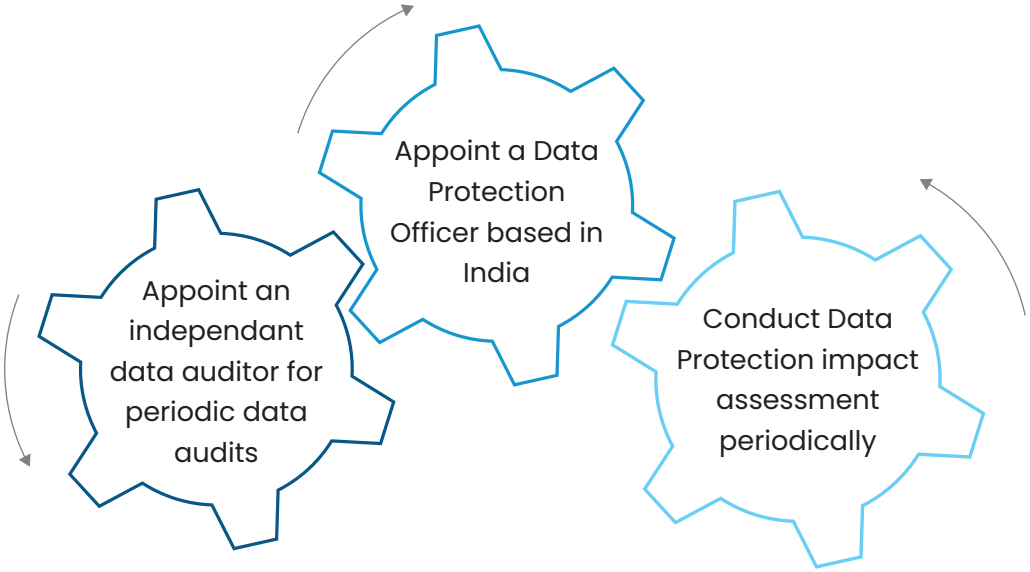
Organizations that process large volumes of sensitive data sets will be declared by the government as Significant Data Fiduciary.

What is sensitive personal data?

Some personal data is considered sensitive, as it could cause harm to the individual if leaked or misused. While each data privacy law may have its nuances, personal data is classified as 'sensitive' if it relates to race, caste, sexual orientation, physical or mental health, criminal offenses, or court proceedings.

Obligations of Significant Data Fiduciaries:

In addition to the general obligations of the data fiduciaries, a Significant Data Fiduciary must also



How do we turn obligation into opportunity?

FMCGs should not view the DPDP Act as a compliance mandate but as an opportunity to enable business innovations, adapt consent architecture and trust framework to control corporate or customer data better, and gain customer trust and loyalty.

Obligations as a Data Fiduciary

- Appointment of a DPO*
- Audits by an independent data auditor*
- Data Protection Impact Assessment*
- Identify and institutionalize basis for processing
- Drive awareness & trainings
- Data breach notification
- Publish business contact information of DPO / Grievance Officer
- Respond to data principal rights requests
- Appoint data processor under a valid contract

Data Management Approach

- Data discovery and classification of personal data
- Inventoryof systems with personal data
- Data Lifecycle management (Collection, Use, Storage, Retention & Deletion)
- Maintain accurate personal data

Data Privacy Requirements

- Implement a consent management framework and system
- Set up privacy notices
- Select tools for cookie and consent management (collection, storage and tracking)
- Refrain processing personal data of child that may cause harm (obtain parental consent)

Data Protection Controls

- Implement data security controls such as data discovery, data classification, data loss prevention, data masking and encryption

Data Transfer Strategy

- Conduct data transfer risk assessments
- Maintain a risk register
- Draftdata transfer agreement templates

Resilience

- Test your incident response, breach handling, executive decision-making
- Cyber Insurance coverage

Key areas to watch out for privacy outcomes before hiring any data processor (WIP)

Today, FMCG companies wield a lot of data through various customer touchpoints for promotional marketing purposes and to deliver personalized experiences. It is imperative to transform the captured data into actionable insights to gain a competitive edge.

But, with the rising operational overhead, workforce, and infrastructural burdens, in-house data processing proves to be a cost-prohibitive proposition for most businesses. And now, with the enactment of the DPDP Act, processing the data while staying compliant has become a crucial factor in avoiding hefty fines.

That's why companies need to turn to data processing experts who play a vital role in data handling and help with data protection compliance, legal and regulatory compliance, maintaining trust and reputation, and safeguarding individual privacy. So, let's understand who is a data processor and how to find the right data processing partner.

Data processors or third-party companies process the company's data on your behalf. They are essential in ensuring the secure and lawful processing of personal data on behalf of companies (data controllers). Their responsibilities include following instructions, maintaining data security and confidentiality, assisting the data controller, subcontracting and data sharing with adequate safeguards, notifying data breaches, adhering to data retention and deletion instructions, and complying with data protection laws.

Therefore, finding the right partner who can process data correctly, help you stay compliant under DPDP, and maintain the trust of data subjects is incredibly necessary. Here are 4 main factors to consider while selecting the right vendor -

1. Ensure Data Security and Privacy -

Data security is non-negotiable today, particularly under privacy regulations such as GDPR and HIPAA, and now with DPDP. Any data processor brought on board must ensure compliance with the DPDP Act and the rules laid out until now.

Other essential factors are data processors' data breach history and residency requirements. Did they have any breach history, and how did they overcome the incident? Do they have any incident response mechanism in place? Additionally, inquire about their data encryption methods, security control measures for customer and transactional data, and overall commitment to maintaining data security.

2. Data Processing Operations

Under the DPDP Act, data controllers must adhere to a few specifications -

- **Data Purpose Limitation and Minimization -** Only collect data for specific, lawful, and legitimate purposes and use that data only for the intended purpose. They may not collect excessive or irrelevant personal data.
- **Consent Management:** It is necessary to seek the consent of individuals before collecting, using, or sharing their personal data.

It is imperative for data processors to help companies adhere to the above salient features of the act, and these things must be included in the tools or platforms that they are going to work with.

A Data Processor must also ensure the data collected is accurate and up-to-date. They must take reasonable steps to correct any inaccurate or incomplete personal data on behalf of the data fiduciary.

3. Industry Expertise and Reputation

Experience, Financial Stability, and Reputation counts! Investigate the provider's track record in your specific industry. Do they have a history of successfully working with businesses similar to yours? The provider's knowledge can make a substantial difference in their service quality.

4. Scalability and Transparency of Communication

Ensure providers can scale their services to accommodate your business's expansion. Scalability is the key to building a long-lasting and flexible partnership. Check out if they are handling data with integrity and confidentiality.

"Hiring a data processor can help companies optimize a proper roadmap for compliance while ensuring business requirements are met in adherence to the law for keeping customer data safe."

Varun Pandey
CTO, and
Chief Security Officer,
FieldAssist.

DPDP in Real Life – Examples and Applications

1. What is the CPG company's responsibility when a customer buys a product online? - Impact of DPDP on Online Transactions

The DPDP Act is a comprehensive law that sets out several rules for collecting, using, and sharing personal data. For example, the bill requires companies to collect data only through consent, ensure data minimization, and focus on storage limitation, i.e., the data is stored only for a specific period.

For example, let's take Whirlpool, where a customer goes online to buy a fridge from their website. Data fiduciary – in this scenario, Whirlpool should collect, use, and share personal data while staying compliant and safeguarding consumer's personal data.

In case Whirlpool is using a third-party distributor for product delivery, the company needs to ensure they have a valid contract under which it is being maintained and ensure that very minimal consumer data is being shared with them. The company also has to make sure that the data processor it hires

"The act demands FMCG brands to strike the right balance between privacy concerns and promotional efforts to foster customer trust and loyalty without infringing on user privacy. Businesses need a change in mindset from Knowing your Customer (KYC) to Knowing their Data (KYD) paradigm."

Sowmya Vedarth
Partner, Deloitte India's Risk Advisory Practice

protects the consumer data while staying compliant.

Under the DPDP Act, companies can process the data for analytics only if they have collected it with proper consent and if the data is adequately anonymized or aggregated to no longer fall under personal data before processing.

For years now, digital businesses have been stuck between a rock and a hard place, trying to balance personalized experiences with the privacy of their customers. The DPDP Act will strengthen India's digital security posture and make it an attractive and safe place for digital business.

2. Is the DPDP rule applicable when the company exports to an NRI in the EU region?

Let's explain the above question with Whirlpool again. For example, if an NRI comes to the website and purchases the product, there are three use cases to be considered to understand the applicability of the law –

1. If the NRI is already in India and making the purchase, then the GDPR and DPDP law will directly apply to the individual.
2. If the NRI is sitting in India and sharing information with the company based out of him, the company has to verify on what basis the information is being collected, where it is being used, and that the NRI has given his data with consent.
3. The third scenario is if Whirlpool, as a manufacturer, sells in India but has no significant office abroad; it just has a branch. In this case, DPDP is still applicable because regardless of whether you are in India or not, the law applies to the residents of India regardless of citizenship.

DPDP is a residential structured-based law that permits personal data transfers outside India except to countries restricted by the Indian government. So, if you are in India and the Indian company is collecting your data, the law is applicable. And, if you are NRI and the Indian company or foreign company is collecting your data – the law is applicable.

3. Can the data processor of a company outside India analyze Indian buyer data while remaining compliant?

It should be clear the processing of personal data by judicial bodies or data processors outside India also partially comes under the law.

For example, suppose Whirlpool hires a data processor located in Turkey in this scenario. In that case, the data processor partner partially comes under the law. However, Whirlpool has to fully adhere to the legislation as a data fiduciary because data is still being collected from India.

The data processor can transfer the data to Whirlpool in India as a local data processor as the law offers extra-territorial scope, i.e., it applies to the processing of personal data outside India (irrespective of the location of the entity processing) in connection with providing goods to data principals located within the territory of India.

However, Whirlpool must also ensure that a proper Data Processing Agreement is signed with the data processor in Turkey in compliance with the DPDP guidance and that it meets all the transfer

requirements, such as ensuring robust data encryption to avoid any breach or leakage.

4. How long can a CPG company store or maintain the user database?

We need to understand that the primary focus of the DPDP Act lies in regulating the collection, storage, processing, and transfer of personal data in the digital landscape. Neither the DPDP Act nor any other law, for that matter, will mandate the storage period, as the storage or maintenance of the data is need-based.

It states that as soon as it is reasonable to assume that (a) the purpose for which such personal data was collected has been met and (b) retention is no longer necessary for legal or business purposes, the Data Fiduciary must cease to retain personal data or remove how the data can be associated with particular Data Principals.

So, the organization must take a call and document the requirements under the Document Record Retention Procedure and justify why they still retain the data collected. And must specify the period up to which it will retain the data collected.

5. How are aggregate and individual data treated under the DPDP Act?

Personal data processed for personal or domestic purposes or aggregated personal data collected for research and statistical purposes not used for any decision specific to a data principal are excluded from the DPDP Act.

If a company can separate individual personal data from aggregated data, it can use it for research purposes. Let's understand this with an example: You browsed the Whirlpool website 10 times and eventually bought the fridge. Now, Whirlpool can analyze the data at an aggregated level to get insights into the sales metrics of that particular product in that particular month.

But if they can track the buyer's personal details and use the analytics for targeted ads, send some coupons, or send some discount SMS, then the company will be liable for non-compliance with the act.

"The act has an inbuilt multi-layered mechanism for addressing grievances. It means YOU and I are in charge of our data, and brands must be transparent about what information is being taken and where and how it will be used."

Amit Kumar
Group Counsel,
DPO (FIP, CIPPE,
and CIPM)

6. Can the same user consent be considered for purchasing another product of the same brand under the DPDP law?

The company has to be precise while collecting the consent as to why they are collecting the consent, and the purpose of the usage has to be stated clearly. For example, the data collected will be used for sales purposes, order fulfillment, etc.

But if you say that the consent is for product X, you cannot use it for product Y. In the company consent policy, brands must be clear about what areas they will cover appropriately.

What's Now, Next, and Beyond

- **Boosts Growth and Innovation**

With the speed of digitization in India and humongous volumes of data being processed, the DPDP Act will empower businesses to safeguard data and boost consumer trust in cross-border trade, supporting India's economy and digital innovation.

- **Empowers Data Principals**

Under the DPDP Act, YOU and I, as individuals, now have the right to manage our personal data, withdraw consent, seek grievance redressal, update our personal info, and appoint a nominee. This empowers Data Principals (consumers and employees alike) to have more control and ensure transparency.

- **Relaxed Cross-border Transfers**

The DPDP Act has provided a minimally restrictive approach to cross-border data transfer, thus reducing costs on transfer mechanisms and significantly boosting profits.

- **Ease in Implementation**

The DPDP Act's phased implementation approach will be effective next year, giving organizations time to redefine their strategies and reduce the resources required to comply with the act.

- **Children's Data Protection:**

The Act puts child gating under 18 years of age for brands to collect and process child-related data. This shift can lead to a more engaged and trusting customer base.

- **Know Your Data to Know Your Consumers**

The KYC-to-KYD approach empowers CPGs to consider the regulatory importance of customer data while ensuring your business meets the Data Protection Act requirements for keeping customer data safe better than your competitors.

Essential Takeaway:

Government compliance is at a tipping point. Regulations are getting tougher, budgets tighter, and the price of compliance is growing! With the evolving regulations, FMCGs/FMCDs must balance privacy and security to stay compliant, avoid hefty penalties, and build trust and loyalty.

As a CPG company, you must protect customers, employees, third parties, or any other data collected by the brand through any touchpoint. Knowing your Data over Knowing your Customers will be the new normal in the coming years!

As digital consumers, under the DPDP Act, you have full rights to know who and how your data is processed. YOU have rights to YOUR data collected by the brand, and if you are not happy with how data has been treated, you can rightfully ask for your data to be deleted.

The DPDP Act is set to commence early this year; therefore, it is yet to be made clear how it will be enforced and what the upcoming risks, rewards, and responsibilities will be. But the message is clear: Consumers want privacy, and CPGs can deliver!

The dexterity, agility, and resilience with which FMCGs will embrace privacy regulations, invest in privacy-friendly technologies, and achieve the goals defined in the DPDP Act will determine their ability to remain fit for the future and contribute to India's transition to a mature digital economy.

2024 will be the start of the new 'Privacy-First' era! And, in this rapidly evolving digital world, adaptation is the key to success, and 2024 promises to be an exciting year in any case.